IT Business Continuity and Disaster Recovery

Tim Bell
IT BC/DR Lead
06/03/2024

IT strategy 2022-2025

Includes as a provider,

- **Recognise operational risks**
  - Define IT-specific policies for disaster recovery and business continuity
- **Enable disaster recovery and business continuity**
  - Enable teams to apply disaster recovery and business continuity policies through dedicated resources, training and senior buy-in to mitigate risks
- **Establish security protocols**
  - Provide the structure to eNsure security policies are implemented with dedicated resources, training and follow-up to reduce associated risks and to preserve CERN's research outputs, past and future

Full IT Strategy document

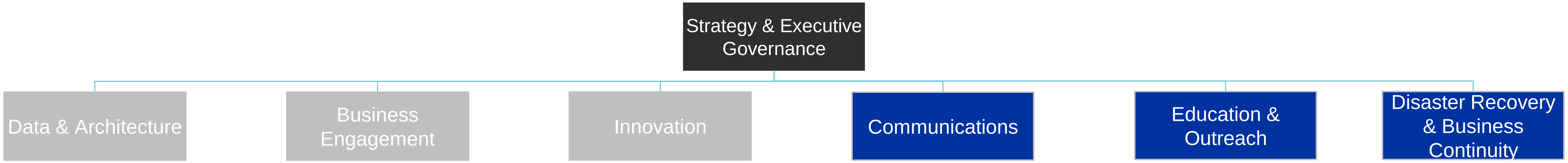
AS-IS External Assessment

Recognise operational risks

Today: IT disaster recovery and business continuity procedures are not adequate. Although failures are limited, the risk is significant to ongoing operations

'We don't have a proper disaster recovery and business continuity plan'

BC & DR lead role



Strategy & Executive Governance Lead

- Drives the development of the IT strategy, together with the IT Department Head, ensuring alignment to CERN's objectives
- Establishes and implements a governance framework, including setting out clear accountabilities across the department and ensuing governance forums are functioning effectively
- Defines and monitors compliance against IT's risk management strategy including response to legal threats, reputational damage and financial risk

Communications Officer

- Oversees all internal and external IT communications, ensuring its messaging is consistent and engaging
- Promotes IT's mission as well as ensuring all messages align to CERN's values
- Prepares detailed reports, press releases, and marketing materials where necessary
- Creates internal communications protocols and initiatives to foster employee moral
- Approves written communications and updates related to service release and change management

Education & Outreach Lead

- Fosters education and training on physics and fundamental research across universities and schools
- Develops a 5 year strategy for Education, including training a future generation of researchers with initiatives such as the School of Computing and CERN openlab Summer Student Programme
- Improves CERN's societal impact through the design and delivery of education and outreach programmes

BC & DR Lead

- **Develops, maintains and organises testing of CERN IT's Business Continuity and Disaster Recovery approach**
- **Supports business planning activities to enable CERN to manage crisis events before they happen and ensure technical capability areas implement defined policies**
- **Oversees the development and implementation of IT risk management policies and plans**

CHANGES FROM AS-IS

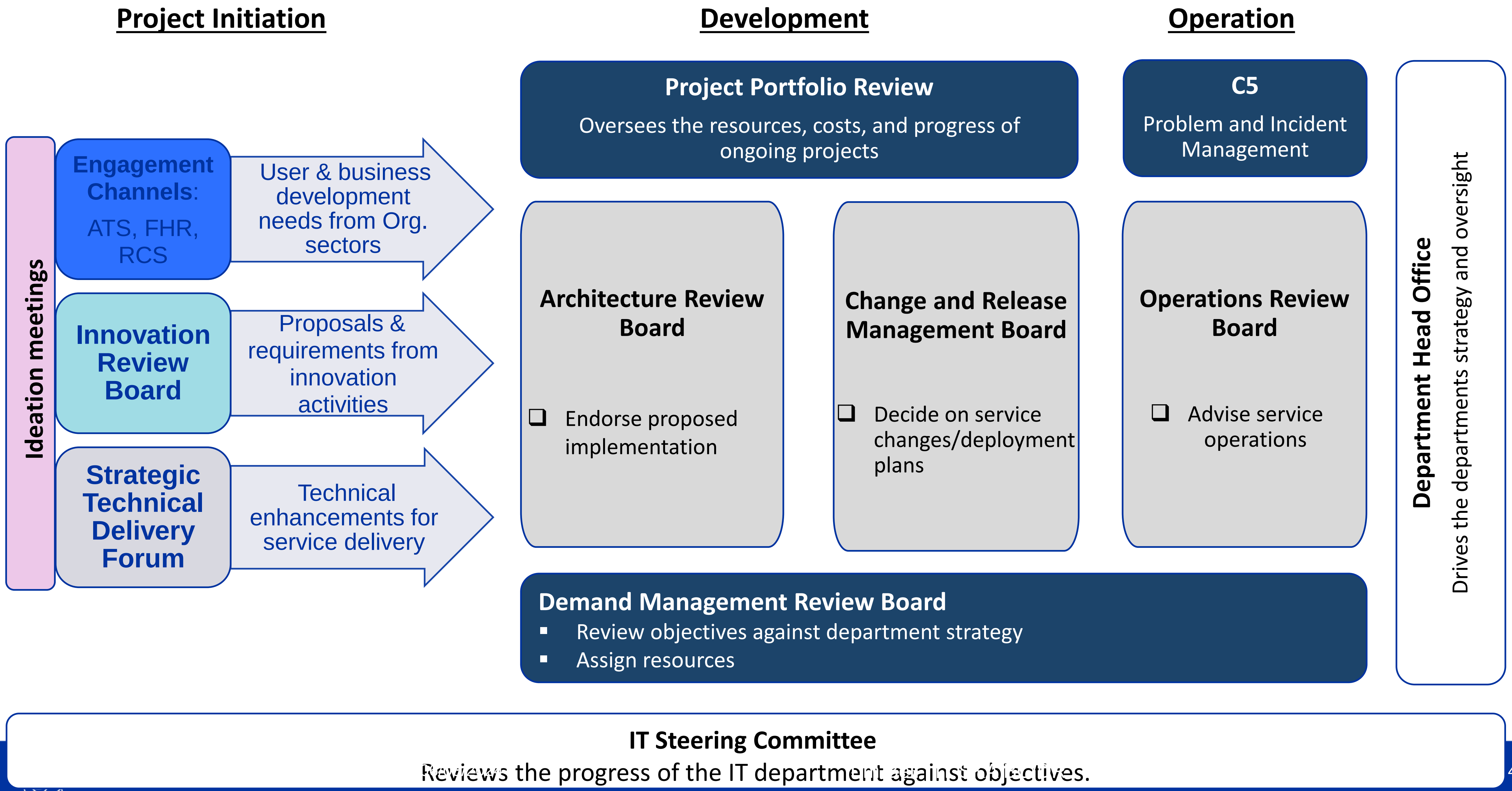
- Creation of an IT Strategy to define the strategic direction of the department in supporting CERN's overall mission
- Implementation of effective governance mechanisms to drive decision making across the department

IMPACT

- Clarity on IT's vision, mission and objectives, promoting increased collaboration and alignment
- Improved decision making and oversight of department performance
- Improved planning and management of educational programs, with higher measurability of societal impact

From IT operating model

Governance Bodies in the Project/Service lifecycle



Project Initiation

Development

Operation

Ideation meetings

Engagement Channels:
ATS, FHR, RCS

User & business development needs from Org. sectors

Innovation Review Board

Proposals & requirements from innovation activities

Strategic Technical Delivery Forum

Technical enhancements for service delivery

Project Portfolio Review

Oversees the resources, costs, and progress of ongoing projects

C5

Problem and Incident Management

Architecture Review Board

❑ Endorse proposed implementation

Change and Release Management Board

❑ Decide on service changes/deployment plans

Operations Review Board

❑ Advise service operations

Demand Management Review Board

- Review objectives against department strategy
- Assign resources

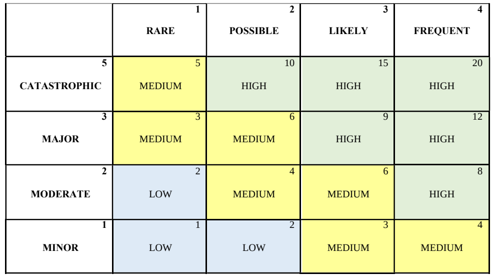
Department Head Office

Drives the departments strategy and oversight

IT Steering Committee

Reviews the progress of the IT department against objectives.

CERN Enterprise Risk Management



	1 RARE	2 POSSIBLE	3 LIKELY	4 FREQUENT
5 CATASTROPHIC	5 MEDIUM	10 HIGH	15 HIGH	20 HIGH
3 MAJOR	3 MEDIUM	6 MEDIUM	9 HIGH	12 HIGH
2 MODERATE	2 LOW	4 MEDIUM	6 MEDIUM	8 HIGH
1 MINOR	1 LOW	2 LOW	3 MEDIUM	4 MEDIUM

- **CERN Enterprise Risk Management has high level risk register**
  - Combines Impact (minor to catastrophic) and Likelihood (rare to frequent) to rank risks

Among the top risks from IT department (2023 rankings):

Risk	Impact	Likelihood
Major infrastructure incident such as fire or flood resulting in substantial loss of computing capacity or data	Catastrophic	Rare
Cyber attack such as compromised accounts leading to data loss, corruption, theft, and the potential inability to perform important function	Catastrophic	Rare
Failure of an important supply or services contract such as company goes bankrupt	Catastrophic	Possible
Human error or malicious actions leading to loss of data and IT services	Catastrophic	Possible
.....		

CERN Crisis Team (policy)

- The aim of the CERN Crisis Management Framework is to assure the most effective response possible to any crisis of significance affecting CERN. The Crisis Management framework focuses on serious, large scale or high impact incidents where a strategic response is required, and details the people and processes required to manage a crisis affecting CERN

- Management will focus on four priorities:

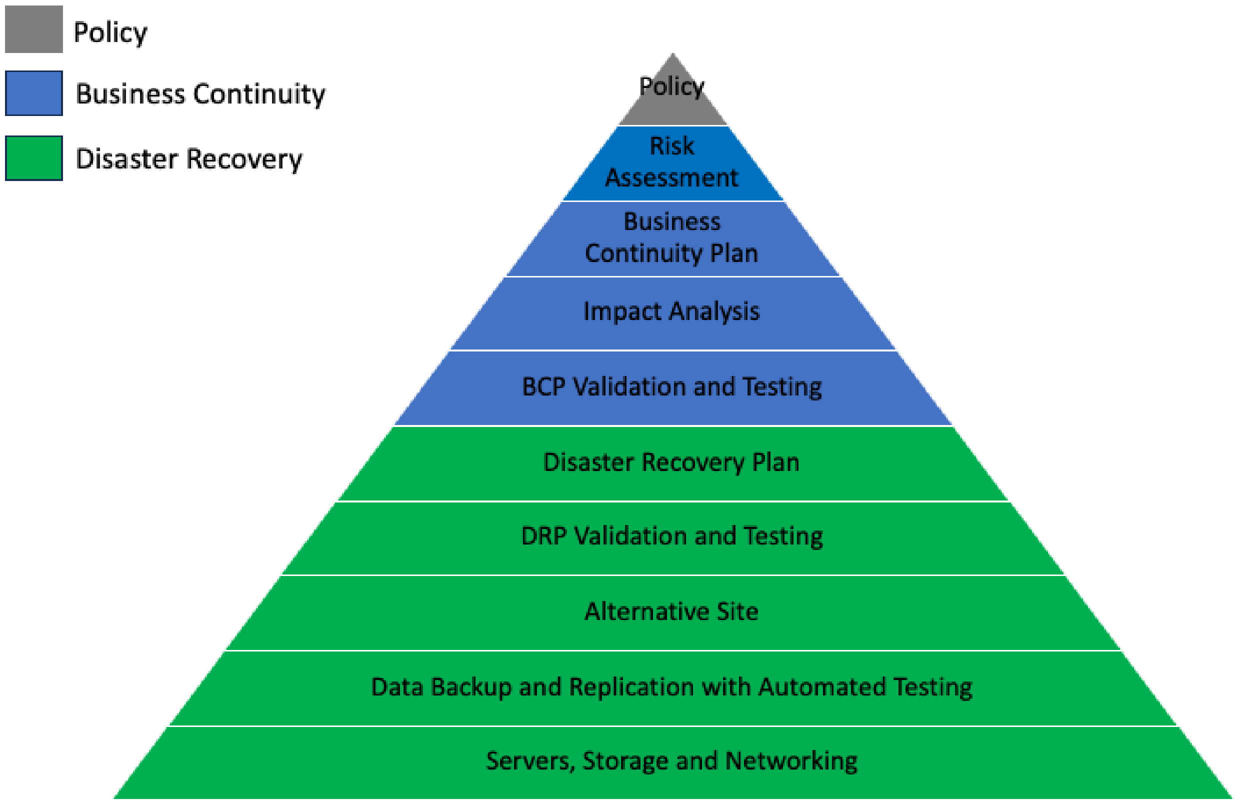
  1. People - Maintaining the health, safety and well-being of CERN personnel, contractors, visitors, local communities, and members of the public on CERN sites.
  2. Environment – Preventing harm or damage to the environment on the CERN sites and in the surrounding area.
  3. Operations – Preventing, minimising, or mitigating the impact on CERN’s activities.
  4. Reputation – Maintaining the integrity of CERN’s image towards internal and external stakeholders.

- 5 activations since 2013 - example would be the building 212 fire in 2019

- Annual tests with a simulated crisis performed and documented

IT BC/DR Policy

- There is currently no organisation wide policy for BC/DR
- The IT department now has a policy approved by the IT department head office in October 2023 including
  - The department should define relevant continuity and recovery planning connected to CERN risk and crisis processes.
  - All continuity and recovery plans should cover essential and critical infrastructure elements, systems and networks, in accordance with key business activities.
  - The plans should be reviewed and tested periodically to ensure that it can be implemented in emergency situations and that the management and staff understand how it is to be executed.
  - All staff must be made aware of the plans and their own respective roles.
  - The continuity and recovery plans are to be kept up to date, taking into account changing circumstances.
  - No goal for Certification but can use criteria for inspiration
- Latest version is here



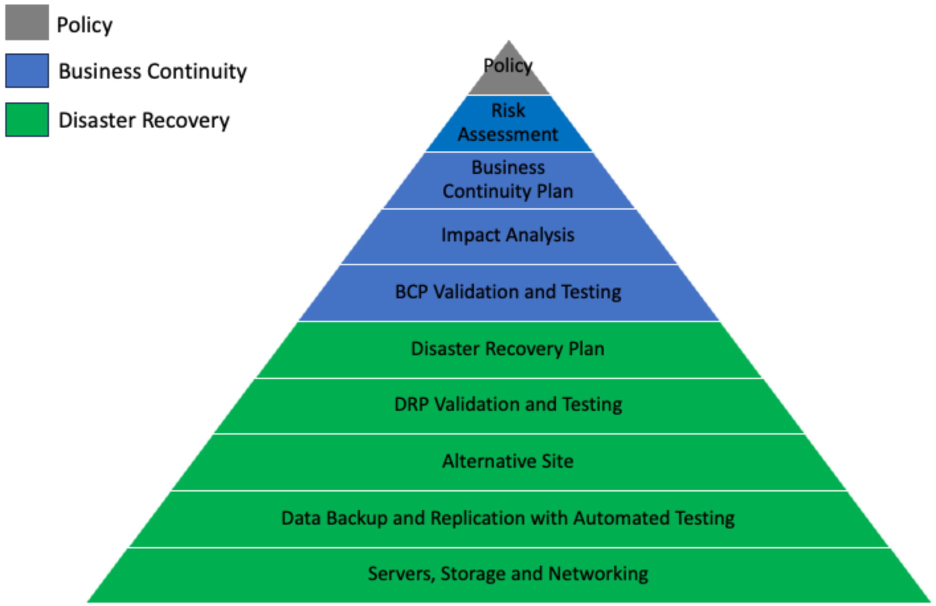
⬛ Policy
🟦 Business Continuity
🟩 Disaster Recovery

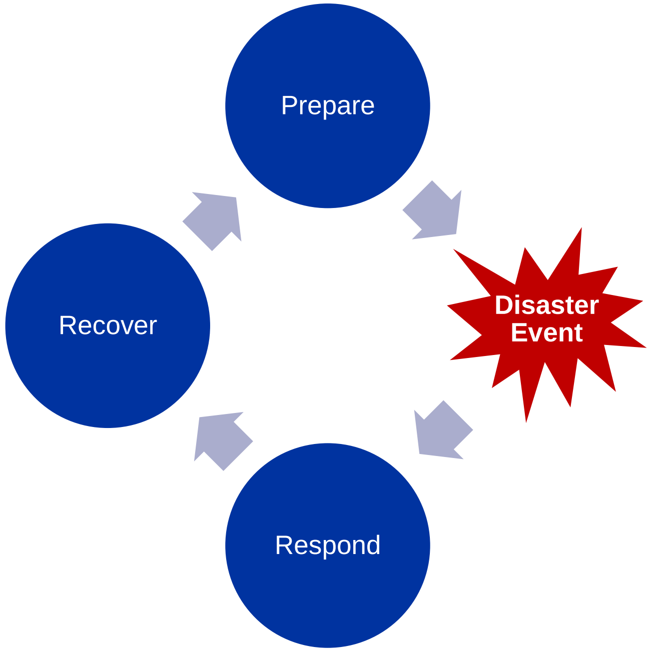
Policy
Risk Assessment
Business Continuity Plan
Impact Analysis
BCP Validation and Testing
Disaster Recovery Plan
DRP Validation and Testing
Alternative Site
Data Backup and Replication with Automated Testing
Servers, Storage and Networking

Business Continuity

- Risk assessment to understand what could go wrong and how likely it would be to happen
- Impact Analysis to understand the damage to the organisation of a process not being able to be performed and which components are needed for a process to be executed
- Business Continuity Plan needs to understand how to limit the damage via mitigations, alternative processes and communications. Latest is here.
- BCP Validation and Testing is to simulate the high impact scenario and ensure the BCP is able to function at the capacity that is needed

Business Continuity is an organisation wide analysis. In the case of IT services being non-functional, this will often involve the business partners applying manual processes and interfacing with the CERN wide Enterprise Risk Management and Crisis Teams.





Disaster Recovery

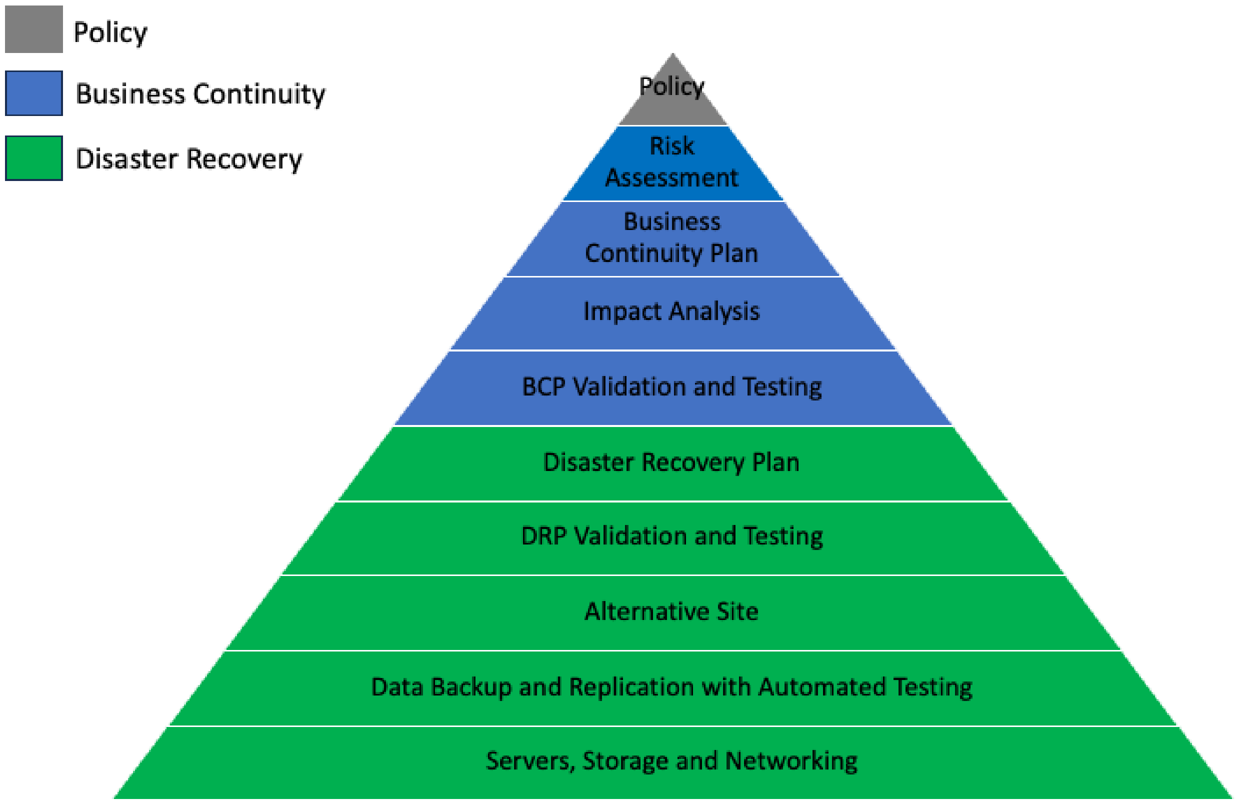
- In the event of a significant incident with an IT service or services, disaster recovery processes return the service to its prior status (with potential downtime and loss of data)

- Depending on the incident, it may involve invoking the recovery for a small set of applications or for an entire site

- Different scenarios will require different recovery plans e.g. corruption of a database with a delayed replica and ransom-ware attack would require two distinct actions

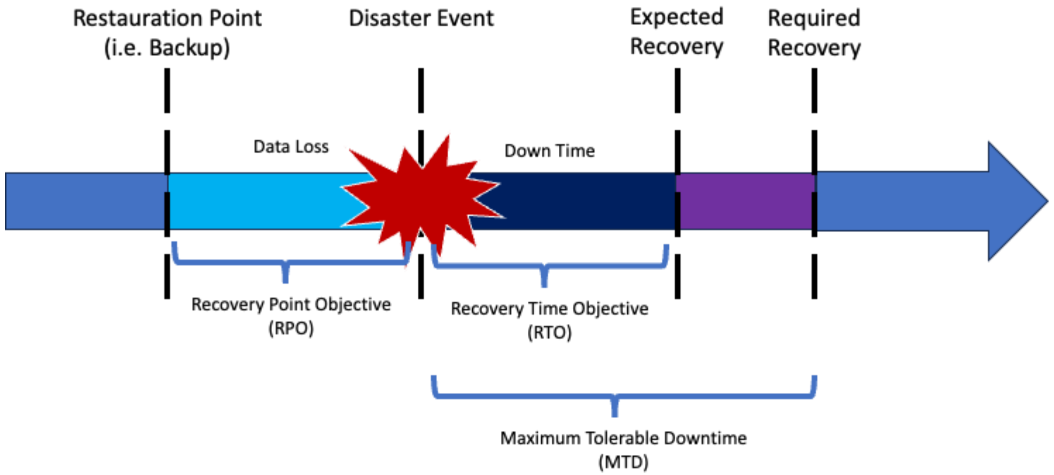
- Planning should cover unavailability of staff, offices or computing facilities

- The only way to validate a disaster recovery plan is by testing such as checking restores of backups, failovers of an application to an alternative site and full disconnect test. Template is here.



Service levels

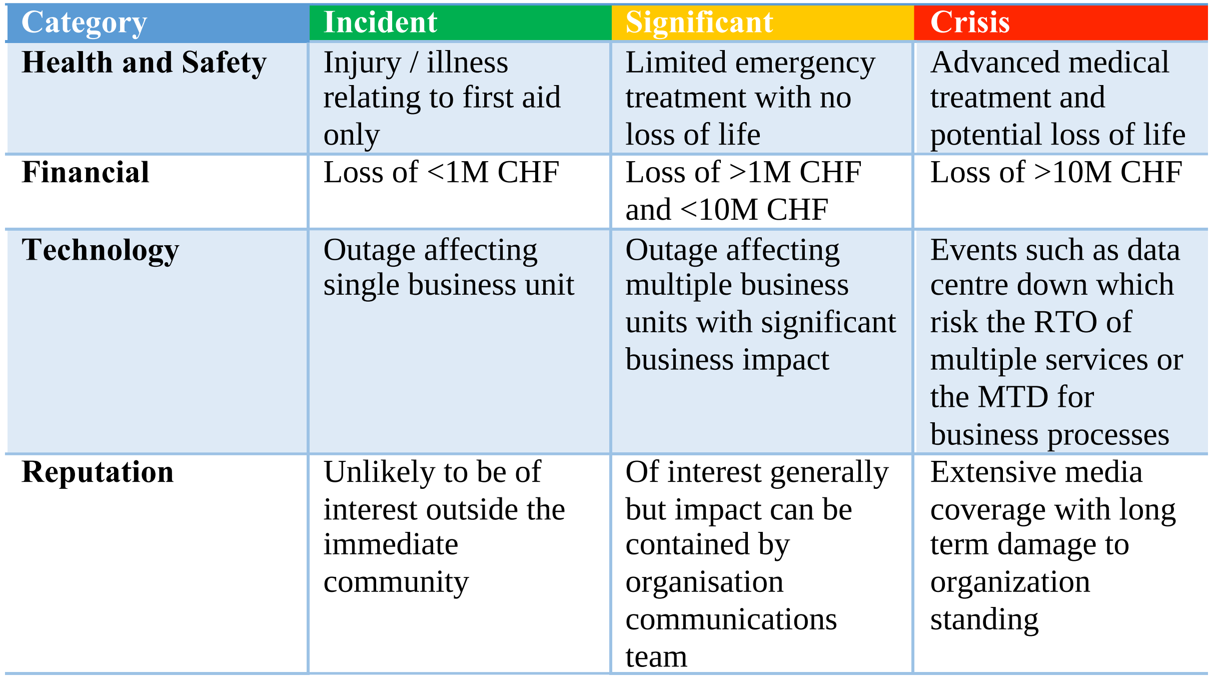
- Service levels as regards BC/DR need to be agreed with the business partners on 3 key metrics
  - Recovery Point Objective is how much data is lost e.g. losing all of today's bookings because the hostel software is backed up during the night
  - Recovery Time Objective is how long does it take to get the service running fully again – business continuity mitigations are needed in the meanwhile
  - Maximum Tolerable Downtime indicates the point where there would be significant harm to the organization's mission
- The desired RPO/RTO/MTD for the business partner is derived from Business Impact Analysis
- The target RPO/RTO is part of the architecture for the IT service
- The actual RTO is obtained by testing
- If the desired and actual are incompatible, a project would be needed to improve the actual or a risk acceptance by the business partner



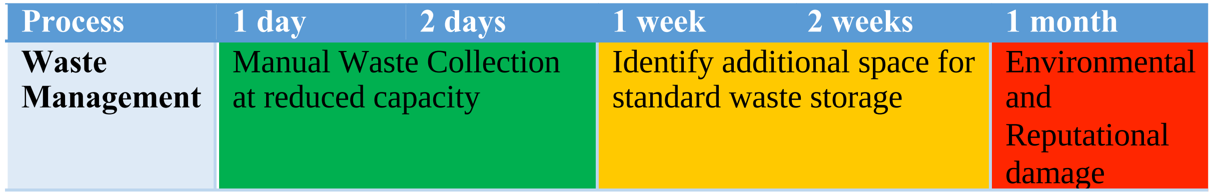
Restauration Point (i.e. Backup)
Disaster Event
Expected Recovery
Required Recovery
Data Loss
Down Time
Recovery Point Objective (RPO)
Recovery Time Objective (RTO)
Maximum Tolerable Downtime (MTD)

Cold	Pilot Light	Warm Standby	Multi Site Active-Active
RTO/RPO : hours / days	RTO/RPO : 10s of minutes	RTO/RPO : minutes	RTO/RPO : seconds
• Less critical systems • Classic restore from backup • Provision and restore after the event • Cost $	• Data live, minimal capacity • Scale out after the event • Cost $$	• Business critical • Initially running at degraded capacity but usable • Scale to full capacity after the event • Cost $$$	• Minimal downtime • Near zero data loss • Mission critical services • Can be complex and potential production impact • Cost $$$$

Business Continuity Management gives trigger criteria



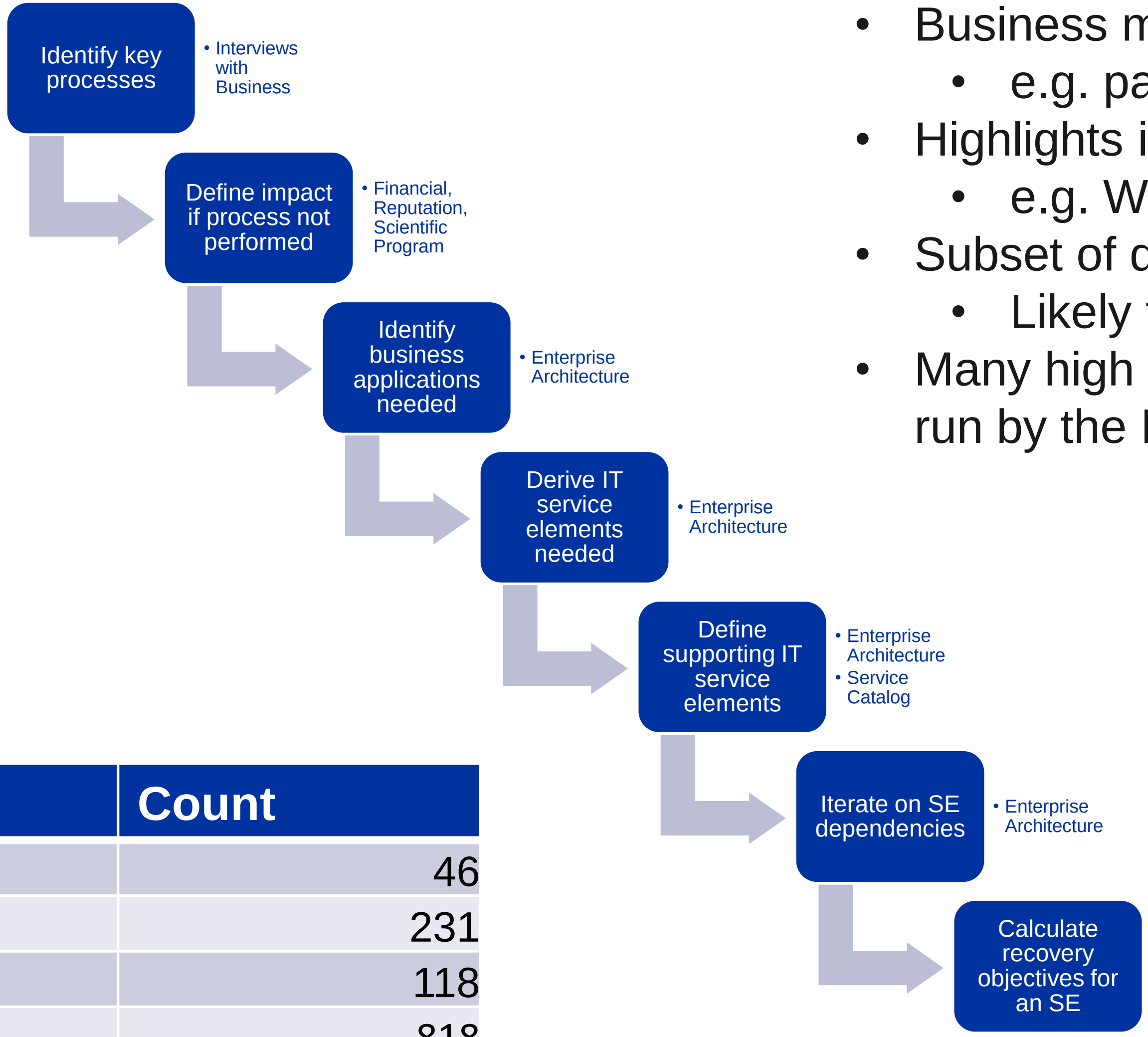
Category	Incident	Significant	Crisis
Health and Safety	Injury / illness relating to first aid only	Limited emergency treatment with no loss of life	Advanced medical treatment and potential loss of life
Financial	Loss of <1M CHF	Loss of >1M CHF and <10M CHF	Loss of >10M CHF
Technology	Outage affecting single business unit	Outage affecting multiple business units with significant business impact	Events such as data centre down which risk the RTO of multiple services or the MTD for business processes
Reputation	Unlikely to be of interest outside the immediate community	Of interest generally but impact can be contained by organisation communications team	Extensive media coverage with long term damage to organization standing



Process	1 day	2 days	1 week	2 weeks	1 month
Waste Management	Manual Waste Collection at reduced capacity		Identify additional space for standard waste storage		Environmental and Reputational damage

- For each business process, define the mitigations (i.e. workarounds) should there be an incident
- Over time, things get worse until there is significant damage to the organisation
- Analysis started in November with Finance and Human Resources, aim to expand this analysis during 2024/2025
- Going Amber is the proposed trigger for the IT BCP to be invoked

Business Impact Analysis



Identify key processes
Interviews with Business
Define impact if process not performed
Financial, Reputation, Scientific Program
Identify business applications needed
Enterprise Architecture
Derive IT service elements needed
Enterprise Architecture
Define supporting IT service elements
Enterprise Architecture
Service Catalog
Iterate on SE dependencies
Enterprise Architecture
Calculate recovery objectives for an SE

- Business mitigations not included
  - e.g. pay the same salaries as last month
- Highlights inappropriate service selection
  - e.g. What does access control need ?
- Subset of data so far (Finance, HR, HSE)
  - Likely to be the most critical
- Many high impact applications are not even run by the IT department

Metric	Count
# Business Functions	46
# Business Applications	231
# IT Service Elements	118
# IT SE SE Dependencies	818

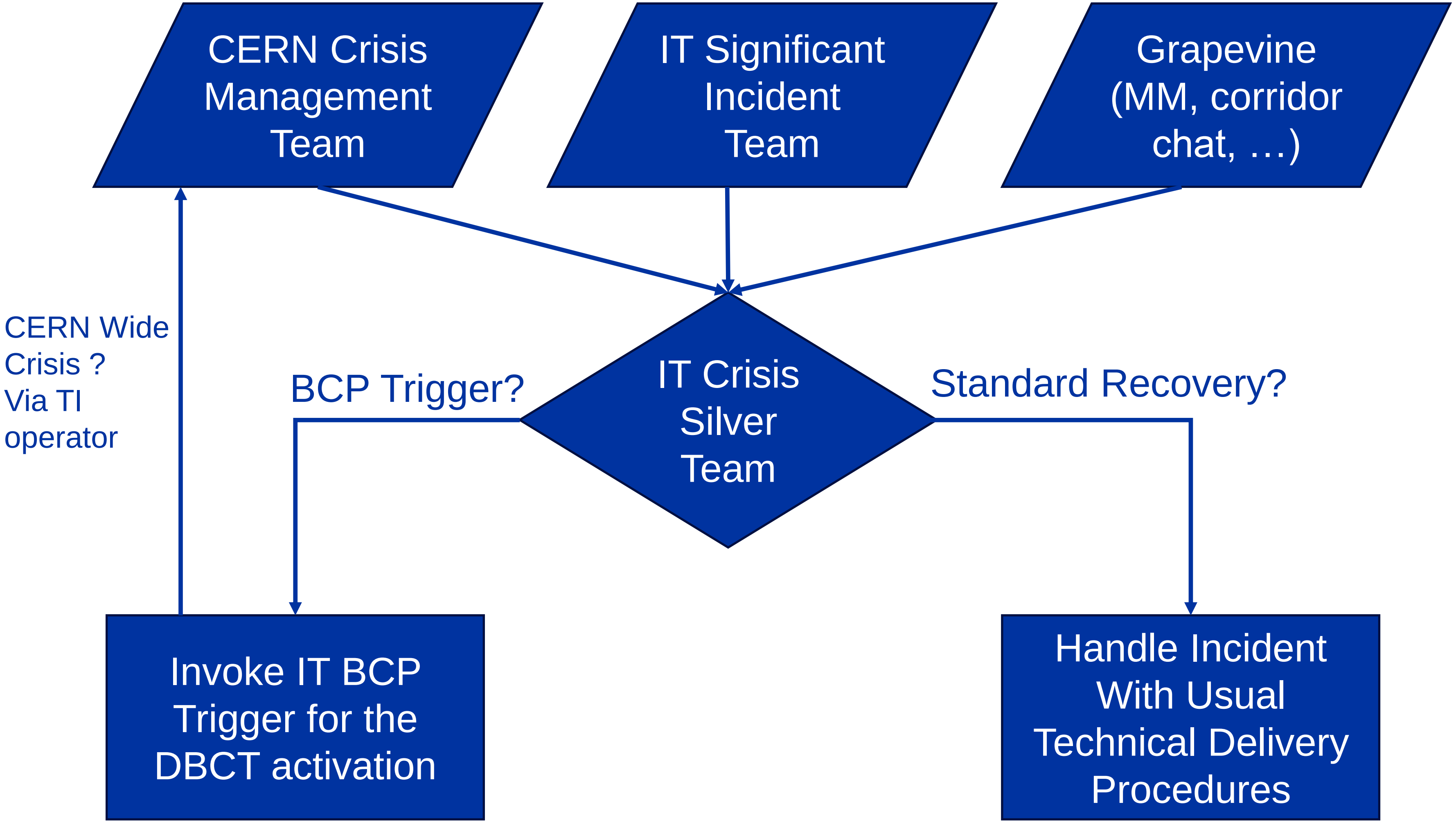
Incidents : some High Energy Physics examples

Incident	When	Site	Details
Tapes 'dampened' due to plumbing mistake	2004	CERN	HEPiX
Tree cuts all power	2005	SLAC	HEPiX
Power outage	2006	CERN	Report
EDH down for 3 days due to RAID failure	2007	CERN	HEPiX
UPS Fire	2009	ASGC/Sineca	Details
20,000 tape files unintentionally deleted	2010	CERN	Details
Site wide power outage	2010	SLAC	HEPiX
Power outage	2014	CERN	Details
Flood of computer centre	2018	INFN	CHEP
Power outage during power test	2021	CERN	ASDF

BC/DR is not only about Fire and Planes

- **Scenarios are evaluated based on past significant incidents. Most likely are**
  - Human error operating an IT system
  - Deployment of an application or system with incorrect logic (including software automation)
  - Component failure (hardware or software)
- **Largest impacts are related to significant multi-service outages with long recovery times**
  - Ransomware
  - Significant infrastructure damage (power, cooling, plumbing)
- **Effort invested in BC/DR can help outside the BCP trigger events**
  - Mitigations (‘How do I post an SSB if SSO is down’)
  - Resilience (‘Are my backups all good in case a user needs files back’)
  - Availability (‘Switch to a read-only clone instance while I do the lengthy production schema upgrades’)
  - Sharing (‘How do we operate a service when the service manager is on holiday’)
  - Flexibility (‘How would we work if the heatwave action plan is invoked’)
  - Channels (‘How to communicate with users if outages occur’)

IT Trigger Event Workflow

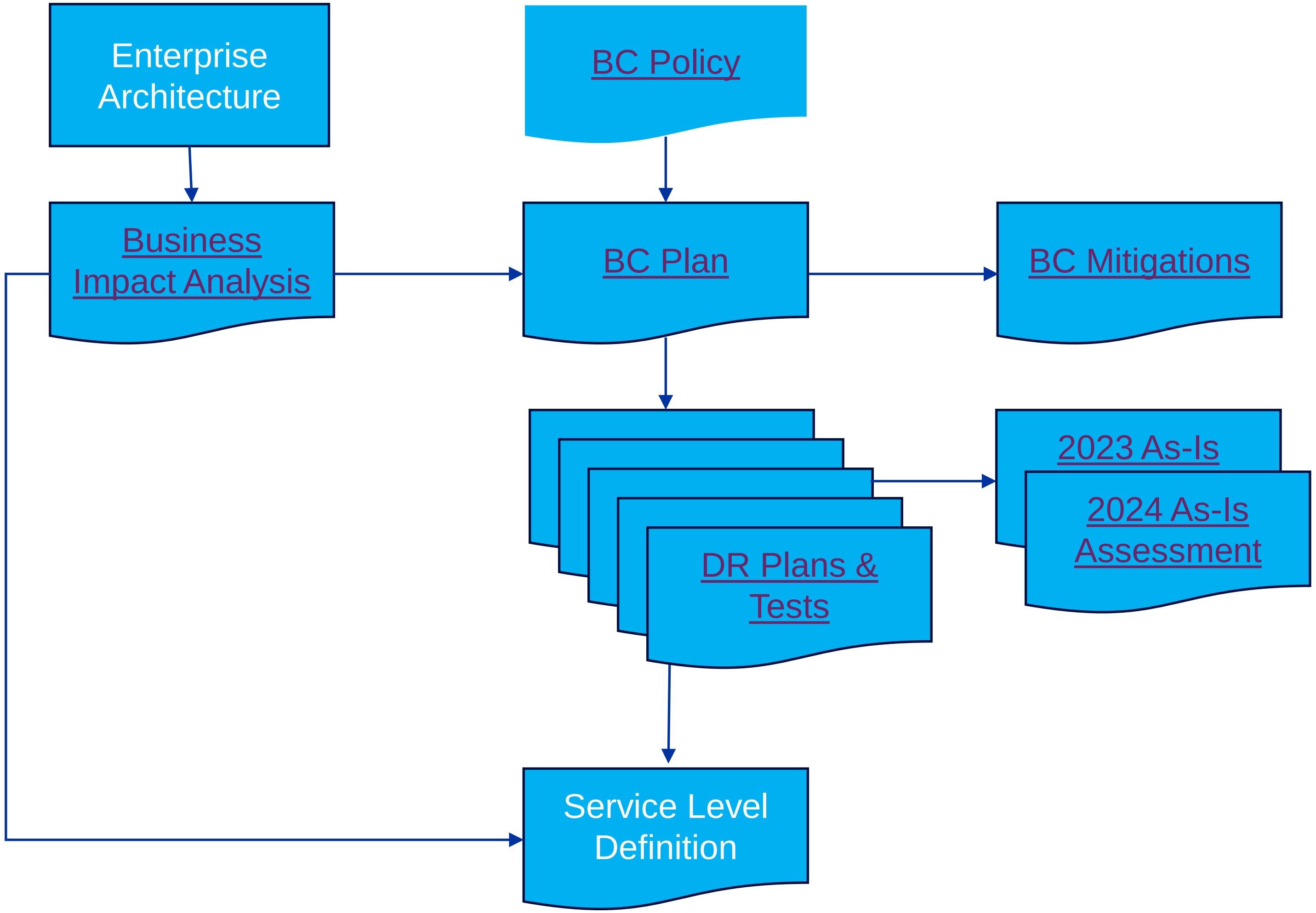

CERN Crisis Management Team
IT Significant Incident Team
Grapevine (MM, corridor chat, …)
IT Crisis Silver Team
BCP Trigger?
Standard Recovery?
CERN Wide Crisis ? Via TI operator
Invoke IT BCP Trigger for the DBCT activation
Handle Incident With Usual Technical Delivery Procedures

- Scenarios may come from multiple sources
- An IT Significant Incident e.g. power loss in B5 may need to be raised to IT management but not a BCP trigger
- IT problems may be elevated to CERN Crisis according to their criteria
  - e.g. legal, reputation
- IT major problems may also be limited in scope to a single service
  - May impact others though

COBIT Maturity Scale and Assessment

Level		Description	DR Summary (IT department average)
0	YOU ARE HERE	Incomplete process	• No testing • No service resilience description
1		Performed process	• Ad-hoc testing (such as ticket handling) • No recovery objectives, no DR plan
2		Repeatable but Intuitive	• Full application cold recovery tested • Recovery architecture defined (cold to active-active) • Estimated recovery times shared with business partners
3	🥉	Established process	• Manually test recovery architecture • Actual recovery times included in service description • DR plan documented and published
4	🥈	Predictable process	• Initiatives to close gap between actual and desired recovery objectives agreed or mitigations by business partners • Recoverability compliant with policy
5	🥇	Optimising process	• DR testing integrated with regular operational procedures • Desired and actual recovery objectives consistent

How BC/DR fits into the IT department services



- **Enterprise Architecture defines processes, teams, applications and how computing systems at CERN connect together**
- **Business Impact Analysis determines effect on the organisation of outages**
- **Service Levels define the commitment to recovery objectives to support the mitigations by the business units**

Disaster Recovery to Prevessin Data Centre

- **Intended for capacity for desired RTO <= 1 day**
  - Environment
  - Safety
  - Access control
  - Short term financial transactions
  - Material damage avoidance
  - Services for rapid recovery (e.g. server administration, source code)

- **Orders placed for 1.8 MCHF, delivery in Q4 2023**
  - 9200 cores, 19 PB (raw) covers the expected capacity above
- **Install in Q1 2024 with aim to be ready for testing Q2 2024**
  - Most applications can be tested in Meyrin Data Centre if ready
- **Suitable for Active-Active and Warm Standby recovery approaches as well as Cold**
  - And may help in non-'Disaster' scenarios also e.g. switch read-only during upgrades, integration testing

Disaster Recovery to Public Cloud

- **Intended for capacity for RTO > 1 day (since <= 1 day covered by PDC)**
  - Not financially viable to have significant resources under-utilised in the PDC for longer recovery time use cases
  - Excluding physics compute and storage (use other grid sites is a better mitigation)
  - Only relevant if the outage is a multi-service, multi-day scenario
  - Approximate capacity needed is 120K cores, 5PB storage
- **Proposal (as discussed with CERN Procurement)**
  - Use of “Accelerated Procedure for Emergency Contracts” (CERN Financial Rules 11.3)
  - Full approval within 4-6 days from CERN Finance Committee
  - Recovery could start immediately within the price enquiry liimits and usage will ramp up
  - Expenditure is O(500K CHF/month) until cause resolved and a 250K CHF one off charge for egress to repatriate the data
- **Testing capacity will come out of cloud contracts O(5K-10K CHF/month)**

Next steps

- **Socialise the establishment of a Business Continuity Network at CERN**
  - Not an IT-only problem and many domain specific standards
  - Business impact analysis needed for the whole organisation (not an IT-only problem)
  - Recent CERN Business Continuity Management System audit is likely to ‘encourage’ this approach
- **Assess IT’s operational resilience**
  - Evaluation of current building blocks and investment in appropriate layers to reduce effort
  - Embed BC/DR into IT’s service lifecycle via architecture and change/release boards
  - Iterate the desired and actual recovery objectives with the user community and define mitigations
  - Formalising Service Levels without cross charging / uplift remains a problem
- **Prepare for DR implementation**
  - Further information gathering and architecture improvements from the IT department
  - Prepare fast recovery infrastructure in the Prevessin Data Centre
  - Training material and building blocks for service managers

Hurdles to be overcome

- **BC/DR standard practise is very oriented towards commercial organisations**
    - A pre-prepared consultancy approach does not work well
- **An organisation wide Business Continuity approach is difficult when departments are independent and there is no CIO**
    - And BC/DR has often not been a priority compared to capability / capacity
    - No financial incentives e.g. reduced insurance if mature
    - Recent CERN audit may ‘encourage’ this approach
- **CERN computing services are often not managed by the IT department**
    - A lot of build-your-own applications which may not have selected the right IT service
    - CERN IT could do better to clearly show the resilience of its services
- **The engineers delivering the IT services are busy**
    - And Disaster Recovery testing is competing with Quantum, Machine Learning and Kubernetes
    - Single expert risk is significant and short term contracts goals do not always include documentation…

Questions?

Backup Slides

BC & DR Team in IT-GOV

BC & DR Team

- Develops, maintains and organises testing of CERN IT's Business Continuity and Disaster Recovery approach
- Supports business planning activities to enable CERN to manage crisis events before they happen and ensure technical capability areas implement defined policies
- Oversees the development and implementation of IT risk management policies and plans

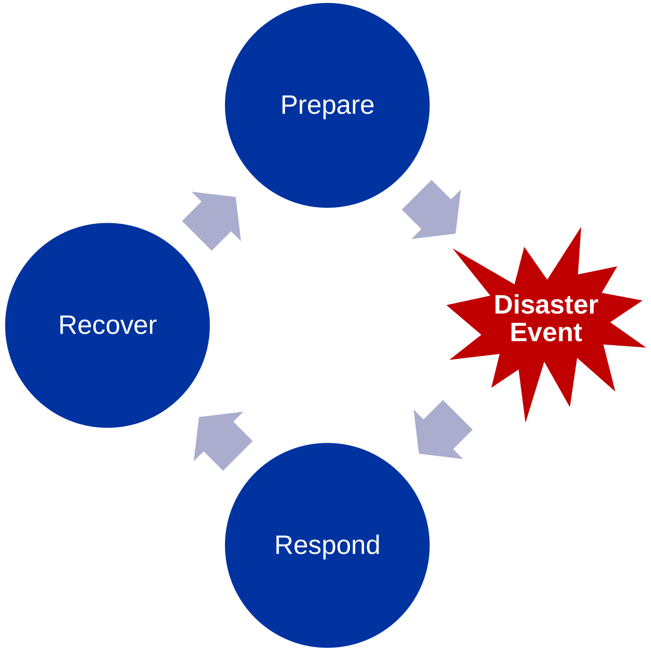
From IT operating model

Tim Bell

Others involved in Risk/BC/DR such as Wayne Salter and Stefan Lueders

Business Continuity Plan (Link)

- **The Business Continuity Plan (BCP) defines the "How" for the IT department and is expected to be a dynamic document**
  - Prepare ("Actions to reduce the length of an outage")
  - Respond ("Steps to perform during the incident to reduce impact")
  - Recover ("How to return to business as usual")
- **Roles with responsibilities listed such as**
  - Department Business Continuity Co-ordinator (DBCC i.e. Tim)
  - IT Crisis Silver Team
  - Department Business Continuity Team (DBCT)
    - Members DBCC, TD GLs, Silver Team …
  - IT Service Managers to prepare with a disaster recovery plan



Using the new operating model to deliver BC/DR (I)

- **With Engagement,**
  - Establish common goals with the sectors on BC/DR (already started with ATS, FHR needed too)
  - Perform impact analysis with business partners to define service criticality
  - Establish service levels with desired and actual RTO/RPO
    - Demand management review board needed where significant effort required (and there will be)
- **With the Project office,**
  - Establish a resource plan and milestones with aim of a testable BC/DR plan for critical processes and IT services, identify additional technical resources needed if building blocks not sufficient
  - Budget planning for people and infrastructure, both regular needs and disaster scenarios
- **With Resource management and Technical delivery,**
  - Identify IT department critical processes and mitigations in the event of system failures for IT Business Continuity
  - Analyse Monthly operations review major incidents for risks, impact and mitigation
    - DR processes can be used to reduce planned downtime impact such as pro-active failover and read-only replicas
  - Plan DR process implementation and testing through the Disaster Recovery Operations in IT team (DROIT)

Using the new operating model to deliver BC/DR (II)

- **With Architecture, Demand management and Change/Release boards**
  - Define criteria for assessment of operational resilience
  - Best practices defined for backup/restore, resource placement and DR testing
  - Reference industry standard DR architecture patterns for service managers
  - Implement the critical improvements for the highest risks within the IT budget

AWS

Cold	Pilot Light	Warm Standby	Multi Site Active-Active
RTO/RPO : hours / days	RTO/RPO : 10s of minutes	RTO/RPO : minutes	RTO/RPO : seconds
• Less critical systems • Classic restore from backup • Provision and restore after the event • Cost $	• Data live, minimal capacity • Scale out after the event • Cost $$	• Business critical • Initially running at degraded capacity but usable • Scale to full capacity after the event • Cost $$$	• Minimal downtime • Near zero data loss • Mission critical services • Can be complex and potential production impact • Cost $$$$

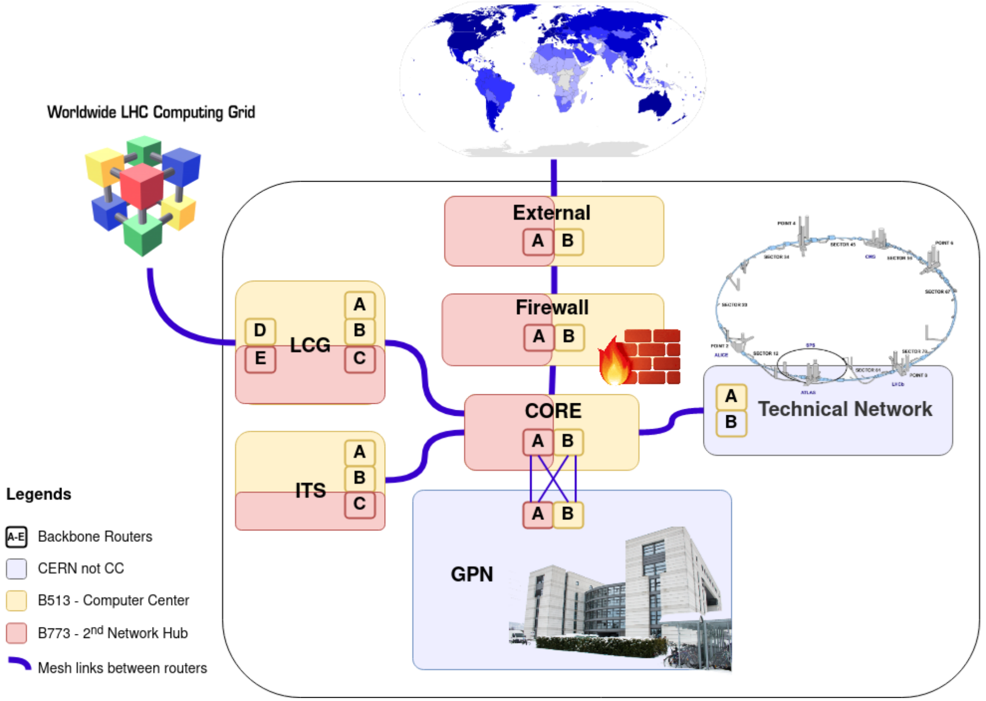
Example: IT/CS’s 2nd network hub tests

ASDF

- **Building 773 provides geographic network redundancy build on backbone components of the network, those connecting only routers.**

- **Comprehensive test plan with documented results, monitoring validation, capacity and service impacts for**

  1. Single router failure
  2. Site router failure
  3. B773 full site failure
  4. (Not performed due to service impact) B513 full site failure



But won’t the PDC solve DR for me ?

- Prevessin Data Centre is scheduled for 2H 2023
  - Providing a low latency near-but-no-too-near computer centre (~4 km)
- It is planned to provide some infrastructure to support disaster recovery, such as
  - VM instances for services (instances in PDC and in Building 513 for active/active)
  - Block/File share storage (in addition to the Object stores/NetApp in the 2nd network hub)

However

- Services need to study best approach (from cold to active/active), implement and test failover
  - Focus on high impact services for CERN with short required RTO (e.g. authentication, safety, access, communications, finance)
  - Resource pools may be different depending on the approach (e.g. public cloud may be affordable for cold, active/active in the PDC will not be affordable for all services)
- BC/DR procedures also needed where we lose some of the PDC or a SaaS service
- DR is not cheap out of the box but disasters cost much more (even the small ones)

DR timeline

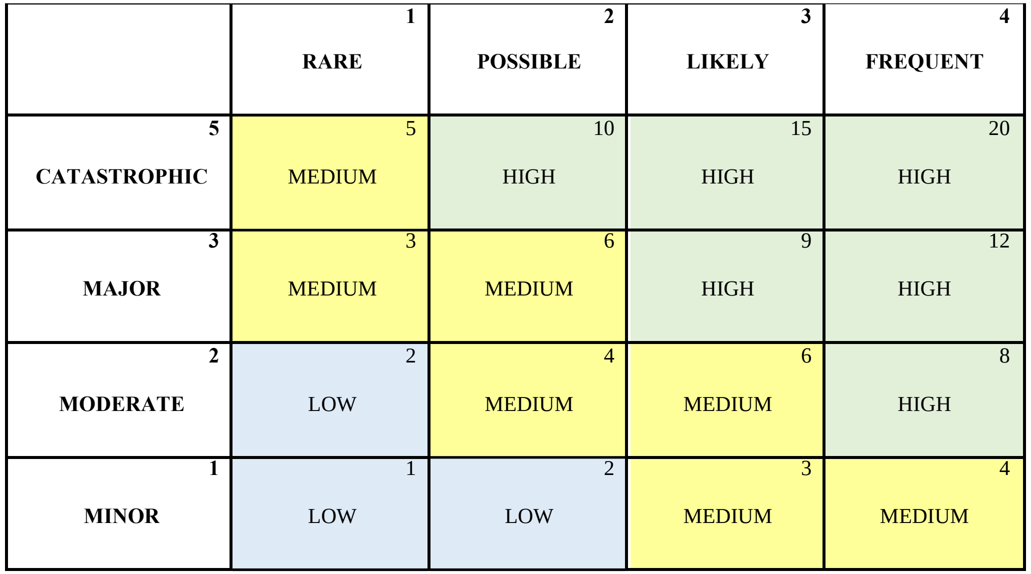
- **DR for IT needs effort from each and every service experts**
  - DR should be part of the service manager responsibilities by default
- **Goal will be to establish common building blocks where possible**
  - e.g. Cloud regions, Storage replication, Database redundancy, Active Directory forests, …

When	What	Who
2H 2023	Assess as-is situation and perform first maturity analysis	BC/DR Team
1H/2H 2024	Perform cold recovery testing and determine actual recovery objectives	All Service Managers
1H 2025	Review mitigation plans with business partners based on the actual recovery times	IT Engagement Channels
2H 2025	Define disaster recovery plans	Auth, Safety, Access, Communications, Financials

Enterprise Risk Management

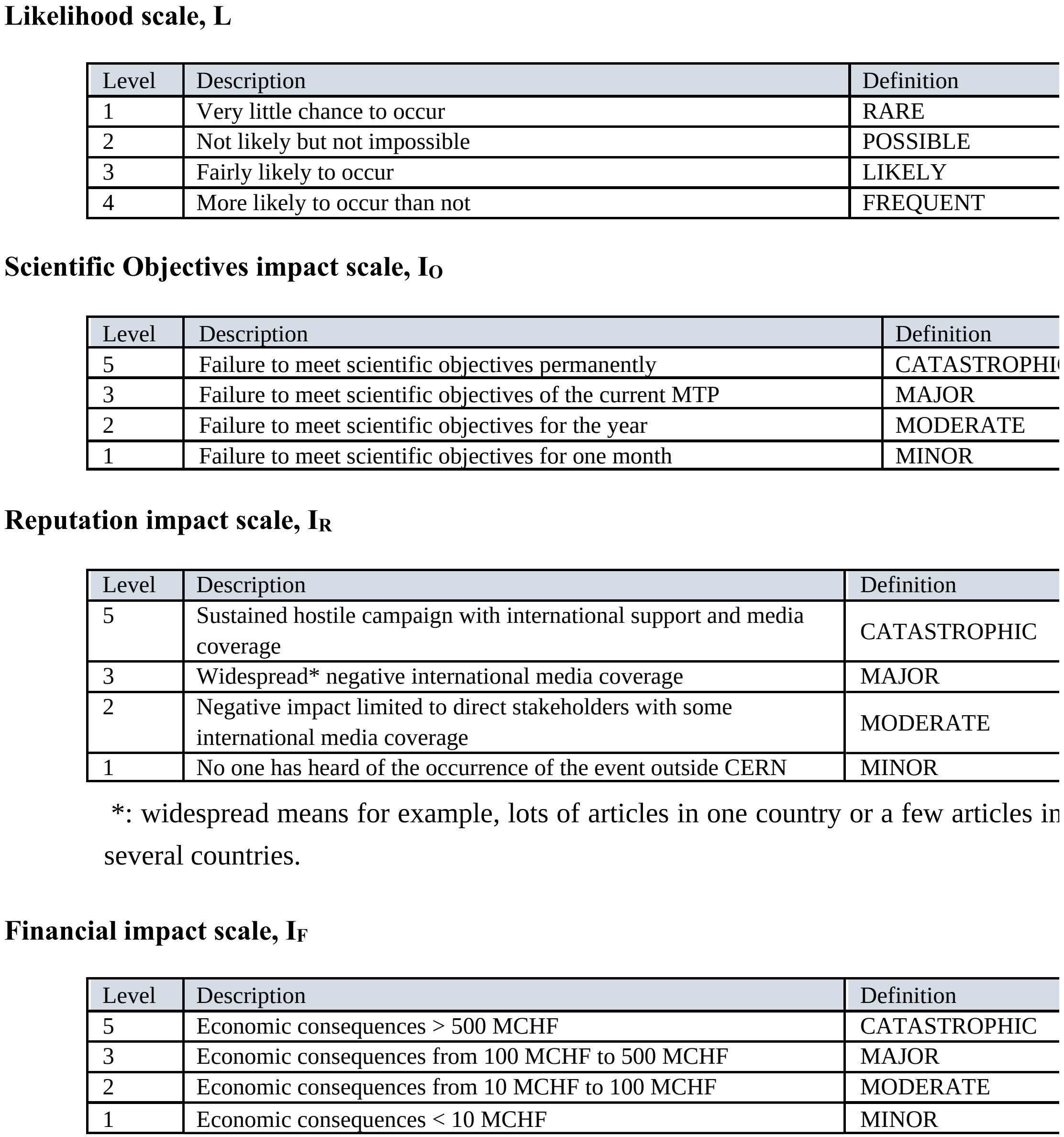
- DG approved the Enterprise Risk Management policy in 2020 (EDMS)
  - “To maintain its position as a leading scientific research centre, and as an exemplary and responsible Organization, CERN must manage the risk associated with its activities. This includes caring for the health and safety of people, the operational efficiency of its installations, and the protection of the environment. In addition, CERN must constantly adapt and strengthen its resilience to adverse circumstances. Enterprise Risk Management (ERM) facilitates decision-making, establishes accountability, and helps CERN to remain an operationally effective Organization.”
- ERM Advisory Committee (ERMAC) established: advises the Director-General on matters relating to the top-level risks for the Organization and on the effectiveness of the risk framework in place. ERMAC helps to ensure that the top-level risks are identified and that controls are in place to mitigate them at the required level.
- Risk register contains **high level** risk descriptions and mitigations, some sample IT ones:
  - Cyber Attack
  - Dependence on unaffordable commercial products and services
  - Failure of important supply or service contract,
  - …

Risk analysis scoring



	1 RARE	2 POSSIBLE	3 LIKELY	4 FREQUENT
5 CATASTROPHIC	5 MEDIUM	10 HIGH	15 HIGH	20 HIGH
3 MAJOR	3 MEDIUM	6 MEDIUM	9 HIGH	12 HIGH
2 MODERATE	2 LOW	4 MEDIUM	6 MEDIUM	8 HIGH
1 MINOR	1 LOW	2 LOW	3 MEDIUM	4 MEDIUM

- Top IT risks are included in the ERM
- However, many IT risks are lower than MINOR (e.g. <10M CHF loss) and thus further study to include a granularity for IT ‘minor’ risks is needed
  - e.g. printer server down means no contractor orders can be executed



Likelihood scale, L

Level	Description	Definition
1	Very little chance to occur	RARE
2	Not likely but not impossible	POSSIBLE
3	Fairly likely to occur	LIKELY
4	More likely to occur than not	FREQUENT

Scientific Objectives impact scale, I_O

Level	Description	Definition
5	Failure to meet scientific objectives permanently	CATASTROPHI
3	Failure to meet scientific objectives of the current MTP	MAJOR
2	Failure to meet scientific objectives for the year	MODERATE
1	Failure to meet scientific objectives for one month	MINOR

Reputation impact scale, I_R

Level	Description	Definition
5	Sustained hostile campaign with international support and media coverage	CATASTROPHIC
3	Widespread* negative international media coverage	MAJOR
2	Negative impact limited to direct stakeholders with some international media coverage	MODERATE
1	No one has heard of the occurrence of the event outside CERN	MINOR

*: widespread means for example, lots of articles in one country or a few articles in several countries.

Financial impact scale, I_F

Level	Description	Definition
5	Economic consequences > 500 MCHF	CATASTROPHIC
3	Economic consequences from 100 MCHF to 500 MCHF	MAJOR
2	Economic consequences from 10 MCHF to 100 MCHF	MODERATE
1	Economic consequences < 10 MCHF	MINOR

CobiT maturity model

Level	Summary	Description
0	Incomplete process	The process is not placed or it cannot reach its objective. At this level the process has no objective to achieve. For this reason this level has no attribute.
1	Performed process	Performed process. The process is in place and achieves its own purpose. This level has only “Process Performance” as process attribute.
2	Repeatable but intuitive	The process is implemented following a series of activities such as planning, monitoring and adjusting activities. The outcomes are established, controlled and maintained. This level has “Performance Management” and “Work Product Management” as process attributes
3	Established process	The previous level is now implemented following a defined process that allows the achievement of the process outcomes. This level has “Process Definition” and “Process Deployment” as process attributes.
4	Predictable process	This level implements processes within a defined boundary that allows the achievement of the processes outcomes. This level has “Process Management” and “Process Control” as process attributes.
5	Optimising process	This level implements processes in the way that makes it possible to achieve relevant, current and projected business goals. This level has “Process Innovation” and “Process Optimisation” as process attributes.

Business Continuity Management gives trigger criteria

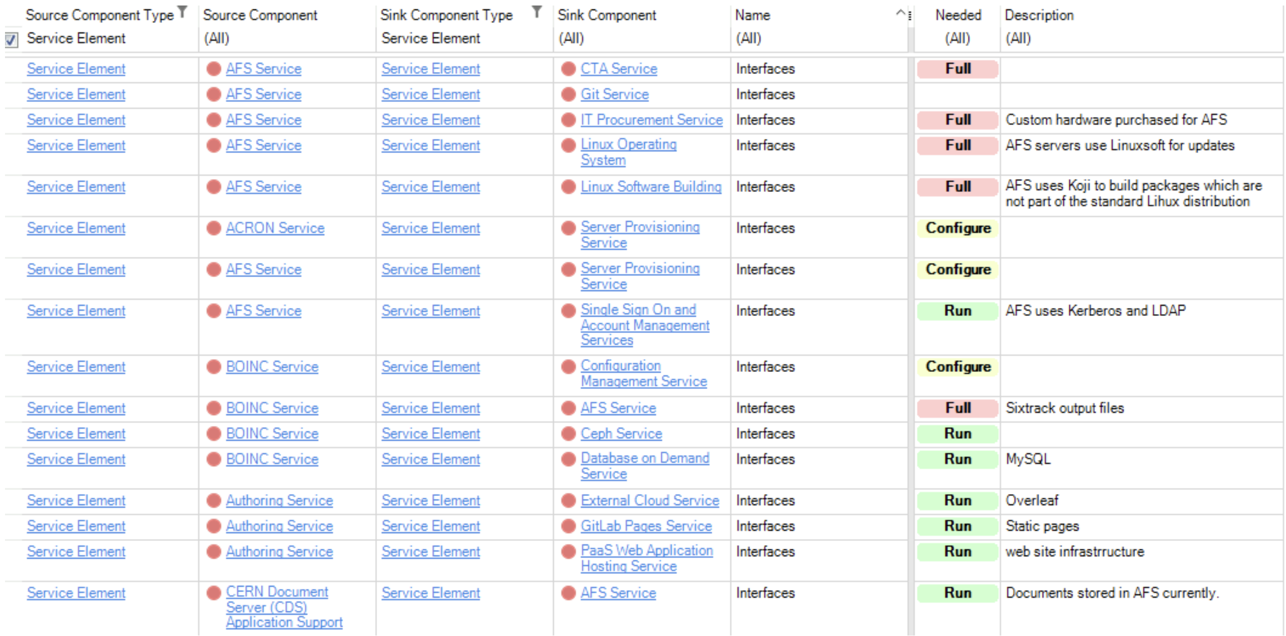
Category	Incident	Significant	Crisis
Health and Safety	Injury / illness relating to first aid only	Limited emergency treatment with no loss of life	Advanced medical treatment and potential loss of life
Financial	Loss of <1M CHF	Loss of >1M CHF and <10M CHF	Loss of >10M CHF
Technology	Outage affecting single business unit	Outage affecting multiple business units with significant business impact	Events such as data centre down which risk the RTO of multiple services or the MTD for business processes
Reputation	Unlikely to be of interest outside the immediate community	Of interest generally but impact can be contained by organisation communications team	Extensive media coverage with long term damage to organization standing

Process	1 day	2 days	1 week	2 weeks	1 month
Waste Management	Manual Waste Collection at reduced capacity		Identify additional space for standard waste storage		Environmental and Reputational damage

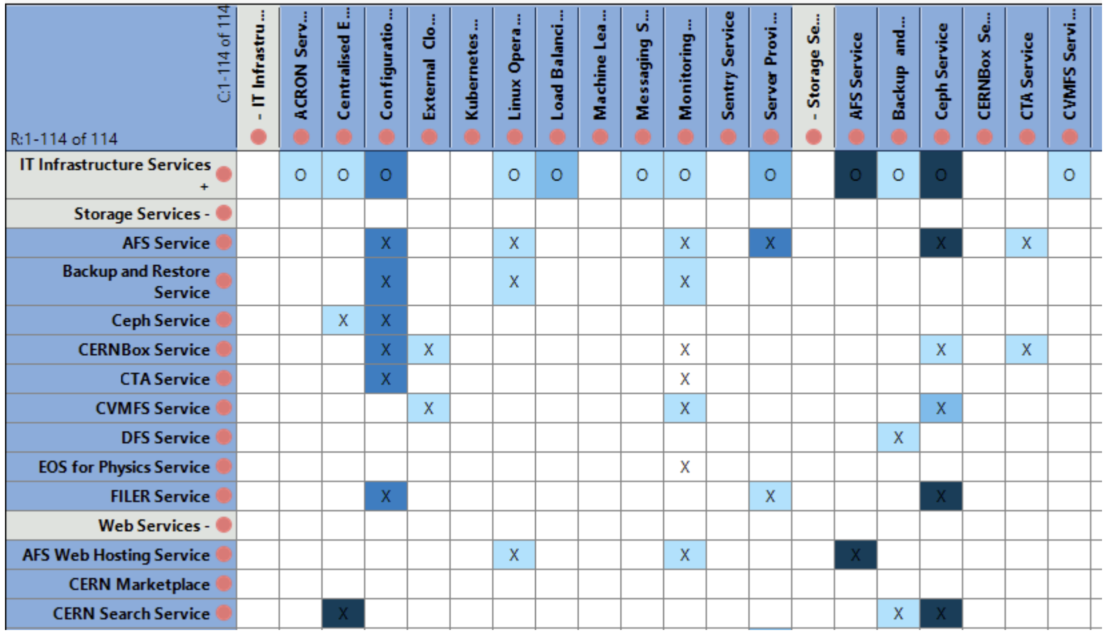
- For each business process, define the mitigations (i.e. workarounds) should there be an incident
- Over time, things get worse until there is significant damage to the organisation
- Analysis started in November with FHR and KPMG consultancy, aim to use same methodology with ATS, HSE and RCS
- Going Amber is the proposed trigger for the IT BCP to be invoked

Dependencies using Enterprise Architecture (I)

- **The IT Service Element dependency data is in the Abacus production model**
  - Including the importance of the dependency from needing for running (e.g. a database) to full (e.g. monitoring), this is color coded in the matrices and additional descriptions
  - Sample data on the Indico page
  - Collected from many sources such as review boards, presentations and C5



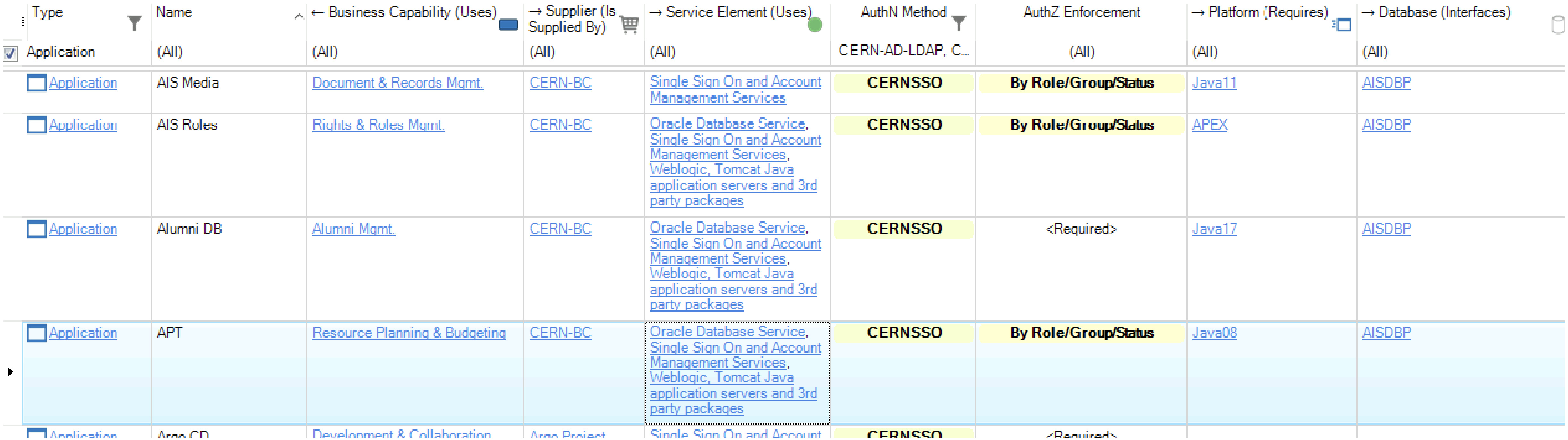
Source Component Type	Source Component	Sink Component Type	Sink Component	Name	Needed	Description
☑ Service Element	(All)	Service Element	(All)	(All)	(All)	(All)
Service Element	● AFS Service	Service Element	● CTA Service	Interfaces	Full	
Service Element	● AFS Service	Service Element	● Git Service	Interfaces		
Service Element	● AFS Service	Service Element	● IT Procurement Service	Interfaces	Full	Custom hardware purchased for AFS
Service Element	● AFS Service	Service Element	● Linux Operating System	Interfaces	Full	AFS servers use Linuxsoft for updates
Service Element	● AFS Service	Service Element	● Linux Software Building	Interfaces	Full	AFS uses Koji to build packages which are not part of the standard Lihux distribution
Service Element	● ACRON Service	Service Element	● Server Provisioning Service	Interfaces	Configure	
Service Element	● AFS Service	Service Element	● Server Provisioning Service	Interfaces	Configure	
Service Element	● AFS Service	Service Element	● Single Sign On and Account Management Services	Interfaces	Run	AFS uses Kerberos and LDAP
Service Element	● BOINC Service	Service Element	● Configuration Management Service	Interfaces	Configure	
Service Element	● BOINC Service	Service Element	● AFS Service	Interfaces	Full	Sixtrack output files
Service Element	● BOINC Service	Service Element	● Ceph Service	Interfaces	Run	
Service Element	● BOINC Service	Service Element	● Database on Demand Service	Interfaces	Run	MySQL
Service Element	● Authoring Service	Service Element	● External Cloud Service	Interfaces	Run	Overleaf
Service Element	● Authoring Service	Service Element	● GitLab Pages Service	Interfaces	Run	Static pages
Service Element	● Authoring Service	Service Element	● PaaS Web Application Hosting Service	Interfaces	Run	web site infrastrructure
Service Element	● CERN Document Server (CDS) Application Support	Service Element	● AFS Service	Interfaces	Run	Documents stored in AFS currently.



C:1-114 of 114 R:1-114 of 114	● - IT Infrastru ...	● ACRON Serv...	● Centralised E...	● Configuratio...	● External Clo...	● Kubernetes ...	● Linux Opera...	● Load Balanci...	● Machine Lea...	● Messaging S...	● Monitoring...	● Sentry Service	● Server Provi...	● - Storage Se...	● AFS Service	● Backup and...	● Ceph Service	● CERNBox Se...	● CTA Service	● CVMFS Servi...
IT Infrastructure Services + ●		O	O	O			O	O		O	O		O		O	O	O			O
Storage Services - ●																				
AFS Service ●				X			X				X		X				X		X	
Backup and Restore Service ●				X			X				X									
Ceph Service ●			X	X																
CERNBox Service ●				X	X						X						X		X	
CTA Service ●				X							X									
CVMFS Service ●					X						X						X			
DFS Service ●																X				
EOS for Physics Service ●											X									
FILER Service ●				X									X				X			
Web Services - ●																				
AFS Web Hosting Service ●							X				X				X					
CERN Marketplace ●																				
CERN Search Service ●			X													X	X			

Dependencies (II)

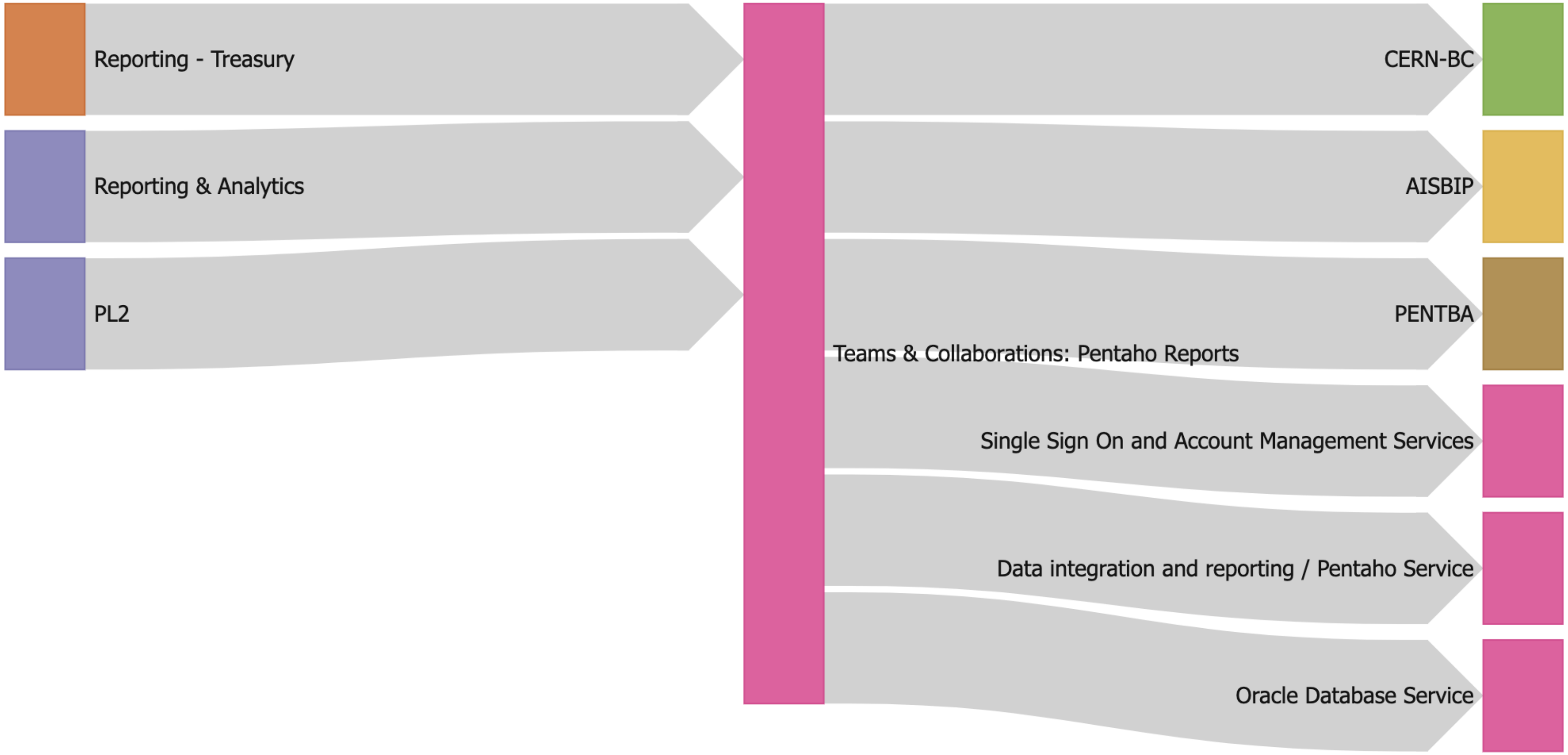
- **Now linked the FAP-BC applications to the associated service elements (e.g. SSO, Oracle, Database on Demand, Tomcat, Pentaho, …)**
  - Support from FHR-IT and ATS-IT Steering Committees to form Enterprise Architecture Forum
  - FHR done, adding Accelerator Sector in H1 2024



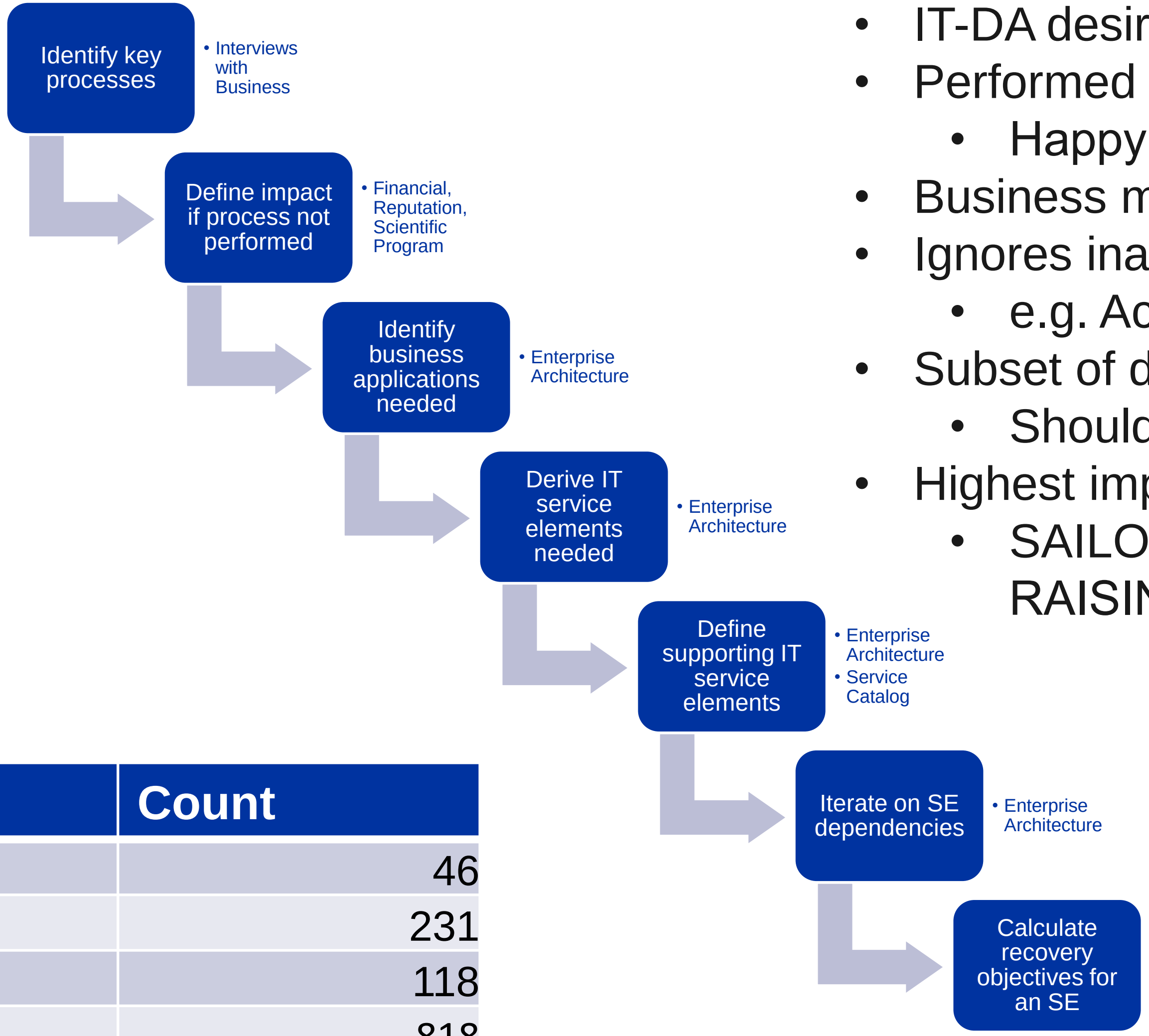
Type	Name	← Business Capability (Uses)	→ Supplier (Is Supplied By)	→ Service Element (Uses)	AuthN Method	AuthZ Enforcement	→ Platform (Requires)	→ Database (Interfaces)
☑ Application	(All)	(All)	(All)	(All)	CERN-AD-LDAP, C...	(All)	(All)	(All)
Application	AIS Media	Document & Records Mgmt.	CERN-BC	Single Sign On and Account Management Services	CERNSSO	By Role/Group/Status	Java11	AISDBP
Application	AIS Roles	Rights & Roles Mgmt.	CERN-BC	Oracle Database Service, Single Sign On and Account Management Services, Weblogic, Tomcat Java application servers and 3rd party packages	CERNSSO	By Role/Group/Status	APEX	AISDBP
Application	Alumni DB	Alumni Mgmt.	CERN-BC	Oracle Database Service, Single Sign On and Account Management Services, Weblogic, Tomcat Java application servers and 3rd party packages	CERNSSO	<Required>	Java17	AISDBP
Application	APT	Resource Planning & Budgeting	CERN-BC	Oracle Database Service, Single Sign On and Account Management Services, Weblogic, Tomcat Java application servers and 3rd party packages	CERNSSO	By Role/Group/Status	Java08	AISDBP
Application	Argo CD	Development & Collaboration	Argo Project	Single Sign On and Account	CERNSSO	<Required>		

Dependencies (III)

- With the dependency data in, the chain from Product to Applications to IT Services/Databases can be visualised (such as from the web interface)


Reporting - Treasury
Reporting & Analytics
PL2
Teams & Collaborations: Pentaho Reports
CERN-BC
AISBIP
PENTBA
Single Sign On and Account Management Services
Data integration and reporting / Pentaho Service
Oracle Database Service

Mini Business Impact Analysis (Link)

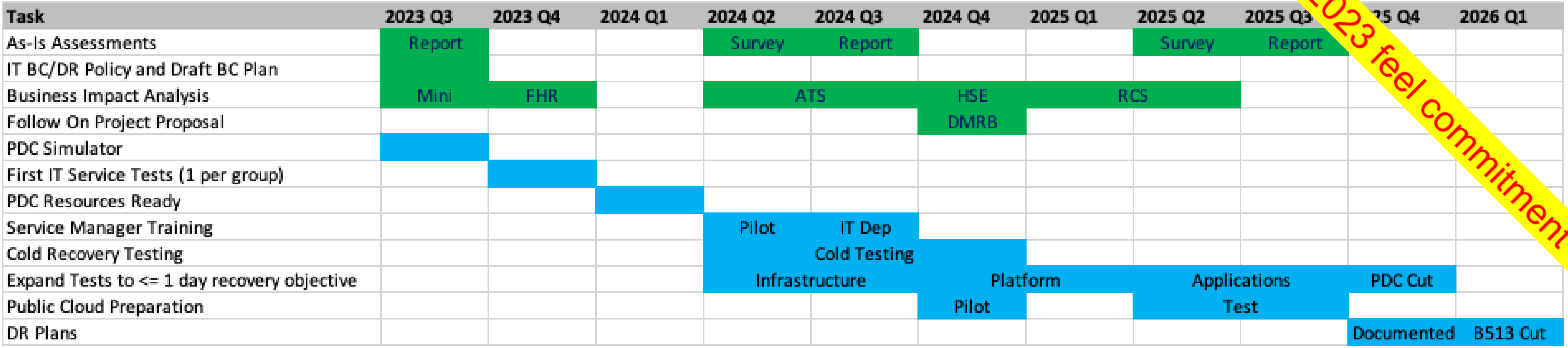

Identify key processes
• Interviews with Business
Define impact if process not performed
• Financial, Reputation, Scientific Program
Identify business applications needed
• Enterprise Architecture
Derive IT service elements needed
• Enterprise Architecture
Define supporting IT service elements
• Enterprise Architecture
• Service Catalog
Iterate on SE dependencies
• Enterprise Architecture
Calculate recovery objectives for an SE

- IT-DA desired objectives are here.
- Performed without interviews
  - Happy to adjust if I've misjudged
- Business mitigations not included
- Ignores inappropriate service selection
  - e.g. Access control needs EOS Web
- Subset of data so far (FHR, ATS, HSE)
  - Should also do this for RCS/IT processes
- Highest impact are often not IT applications
  - SAILOR, NEDAP. REMUS, CSAM, RAISIN, WinCC, …

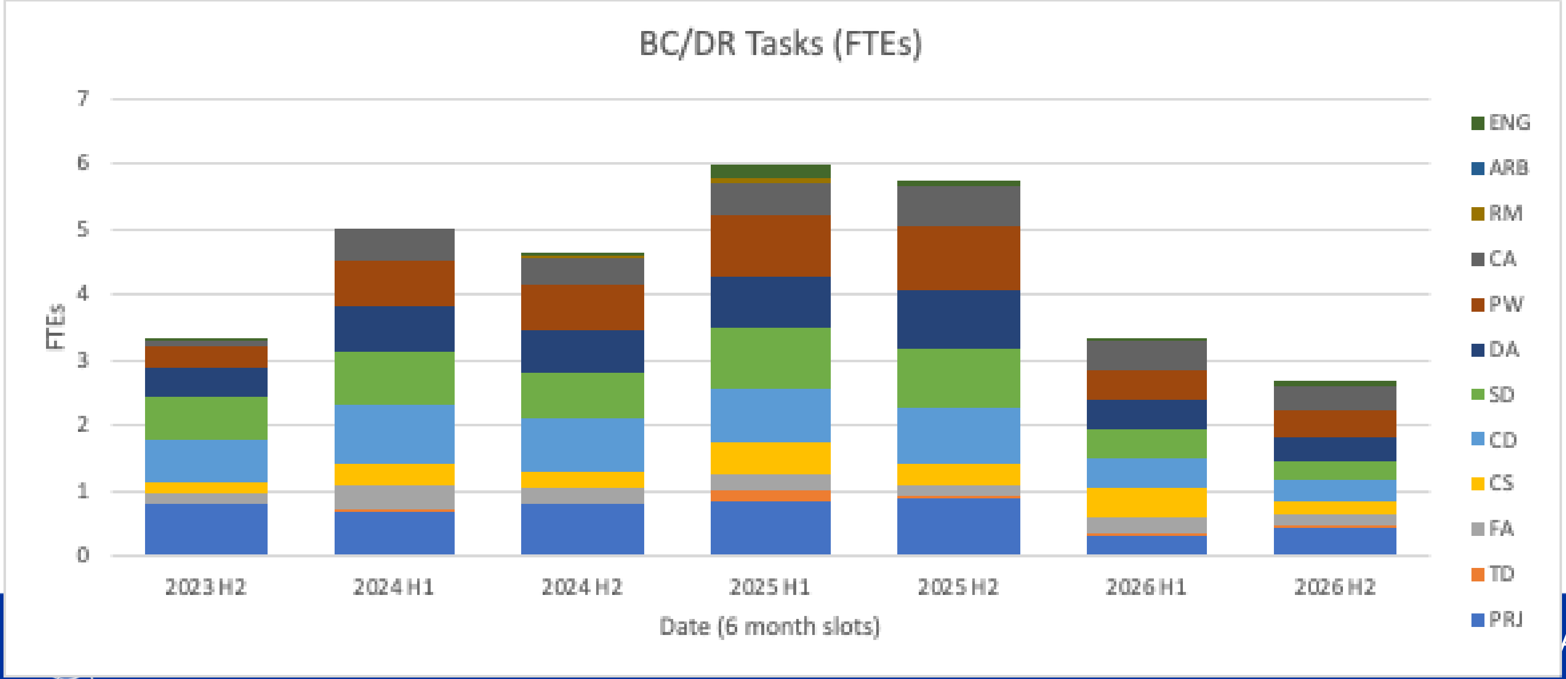
Metric	Count
# Business Functions	46
# Business Applications	231
# IT Service Elements	118
# IT SE SE Dependencies	818

Work Plan to achieve Silver (COBIT 4) (Sheet Schedule)

IT PoW 2023 feel commitment too high



Task	2023 Q3	2023 Q4	2024 Q1	2024 Q2	2024 Q3	2024 Q4	2025 Q1	2025 Q2	2025 Q3	25 Q4	2026 Q1
As-Is Assessments	Report			Survey	Report			Survey	Report		
IT BC/DR Policy and Draft BC Plan											
Business Impact Analysis	Mini	FHR		ATS		HSE	RCS				
Follow On Project Proposal						DMRB					
PDC Simulator											
First IT Service Tests (1 per group)											
PDC Resources Ready											
Service Manager Training				Pilot	IT Dep						
Cold Recovery Testing					Cold Testing						
Expand Tests to <= 1 day recovery objective				Infrastructure		Platform		Applications		PDC Cut	
Public Cloud Preparation						Pilot		Test			
DR Plans										Documented	B513 Cut



- Resources needed are, generally, expert service managers with knowledge of how services are installed and configured
- Current maturity limits options to delegate to more junior staff
- FTEs does not include linked activities such as Enterprise Architecture, Service Levels or Business Partner effort

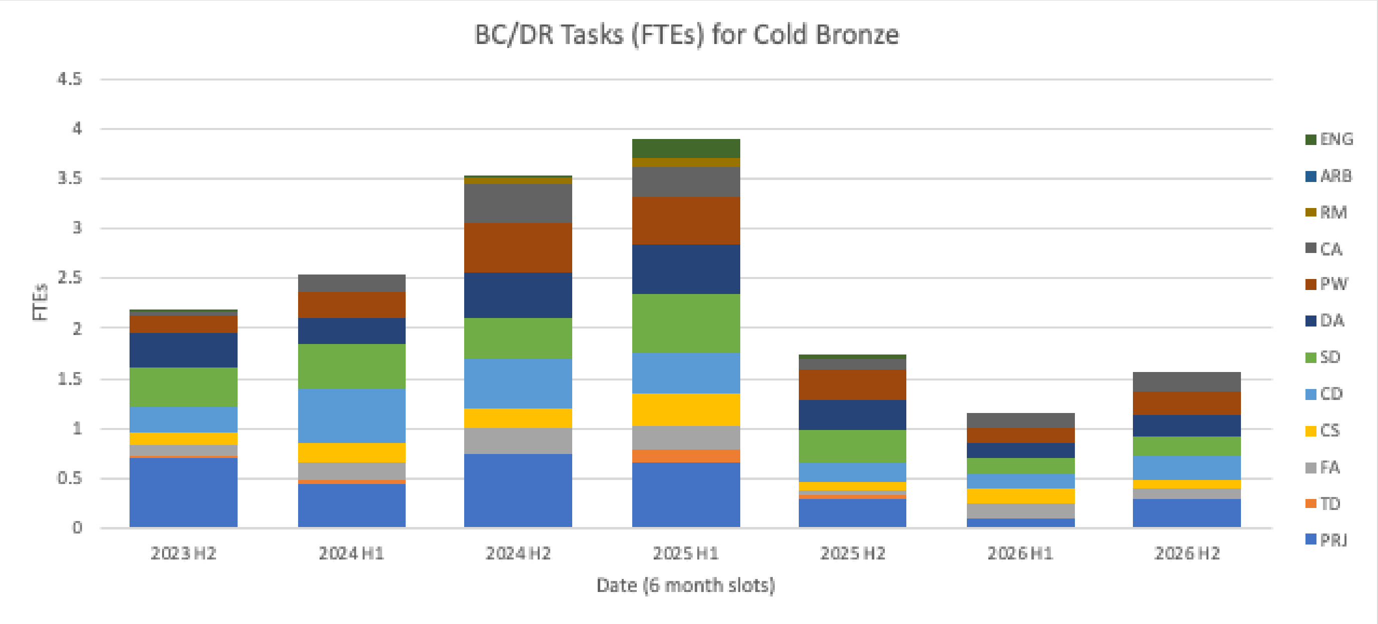
Cold Bronze Work Plan (with major BP mitigations)

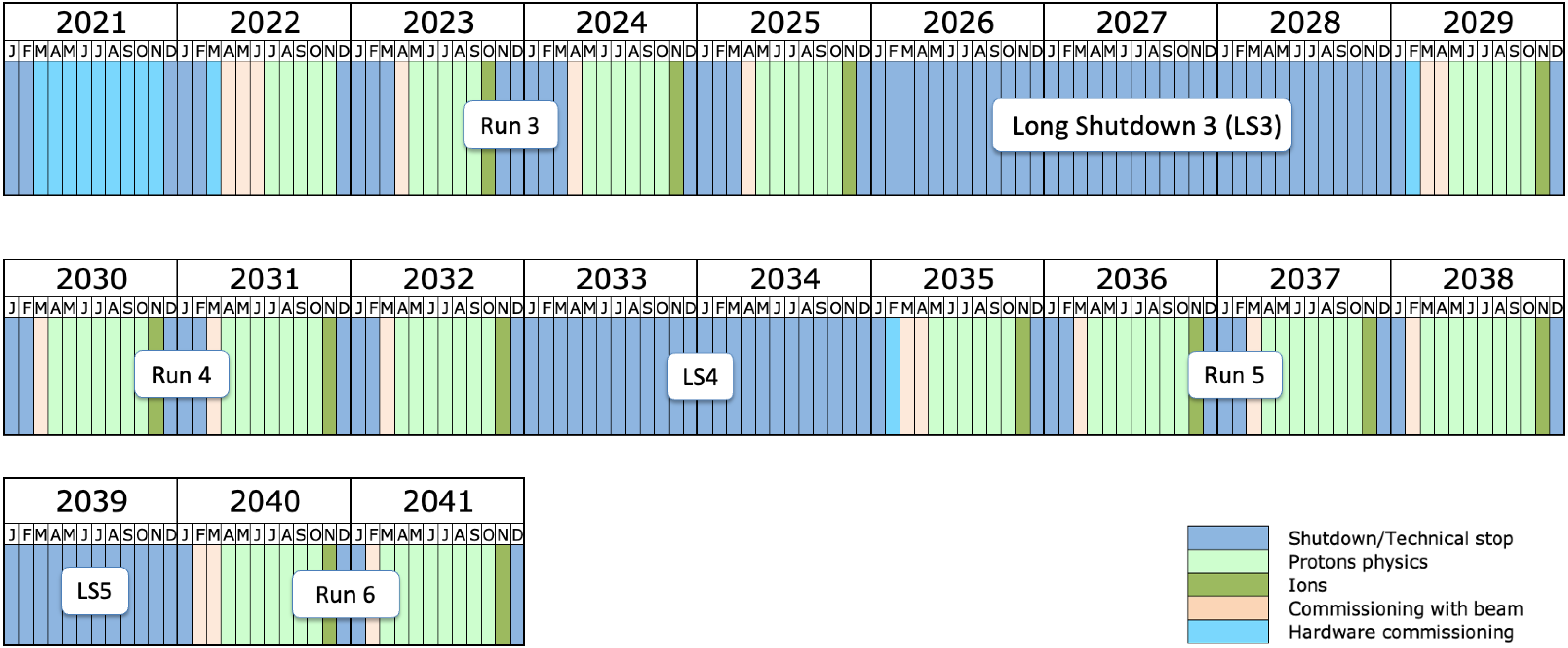
Agreed at IT PoW 2023 for planning

- **Prepare and respond steps as for Silver (i.e. Business Continuity part remains the same)**

- **Investment in Recover steps reduced at the expense of recovery time and major mitigations by user community**
  - Unavailability may be mitigated but data loss is permanent
  - Cold recovery procedures defined, tested and documented (Expert STAF mainly needed – FELL resources would continue to work on building blocks). Business partners informed to plan mitigations accordingly – dRTO will be much shorter than aRTO
  - Bi-annual cold testing, no active-active or warm standby in the short term i.e. many aRTOs will be multi-days/weeks, but carry on FELL work

- **No multi-service outage scenarios to be tested soon (but lower likelihood) – risk acceptance needed**
  - No planned public cloud recovery testing, no disconnect testing before at least 2028 (end LS3) or 2033 (start LS4)





Last update: April 2023

https://lhc-commissioning.web.cern.ch/schedule/LHC-long-term.htm

Standards

There is currently not an agreement to use any specific standards at CERN but these are the ones that have been raised in discussions. The current position is that it is unlikely to be affordable to comply with the entirety of these standards or ensure appropriate certification/actions in a timely manner. However, these can potentially be used as inspiration for some directions to be taken for an organization such as CERN.

Standard	Description
ISO 31000	Risk Management
ISO 22301	Business Continuity
ISO 27001	Disaster Recovery

CERN

home.cern